Examiner's Amendment

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Attorney Jonathan M. Harris on December 2, 2008.

The Claims have been amended as follows:

1. (Currently Amended) A method for compiling parser scripts each corresponding to the structure of security data received from a network component comprising the steps of:

a) when executed by a computer, identifying sets of data categories, each set corresponding to security data received from one of a plurality of network components;

b) when executed by a computer, constructing database record definitions, each defining a record subdivided in accordance with one of the sets of data categories;

c) writing parser scripts that receive security data from the network components and output records, each record corresponding to one of the record definitions;

d) storing said parser scripts;

e) determining the format of each category in said sets; and

f) formatting the subdivisions to match the formats of the categories of the set to which the definition corresponds; and wherein each of the output records of step (c) correspond in format to one of the record definitions.

2. (Canceled).

3. (Original) The method of claim 1 further comprising the steps of:

g) building database tables in a relational database each having the fields of one of the database record definitions; and

h) inserting output records received from the parser scripts into the tables.

4. (Currently Amended) The method of claim [2] 1 further comprising the steps of:

i) building database tables in a relational database each having the fields and formats of one of the database record definitions; and

j) inserting output records received from the data interface operating per defined data constructs into the tables.

5. (Original) The method of claim 1 wherein: at least one of the sets of data categories is identified, at least in part, from the product specifications of the network components.

6. (Original) The method of claim 1 wherein: at least one of the sets of data categories is identified, at least in part, by applying a Management Information Base (MIB) integrator to a Management Information Base for the corresponding network component.

7. (Currently Amended) An information network security data compilation system, comprising:

a) a first network component;

b) a second network component;

c) a third network component; and

d) when executed by a computer, a data parser that is coupled to the first and second network components ~~have~~ has access to a first parser script and a second parser script, the data parser is operable to produce categorized data from the data received from the first and second network components data interface operating with the first and second parser scripts, respectively;

b) when executed by a computer, a second data parser that is coupled to the third component has access to a third parser script, the second data parser operable to produce categorized data from the data received from the third network component with the third parser script; and

c) a relational database coupled to the first and second data parsers.

8. (Original) The data compilation system of claim 7 wherein:

a) the first network component is a firewall and

b) the second network component is an intrusion detection system.

9. (Original) The data compilation system of claim 7 further comprising:

a) a third network component and

b) a distributed data manager; and wherein: the data parser is coupled to the second and third network components through the distributed data manager which collects and compresses data from the second and third network components and forwards the compressed data to the data parser.

10. (Canceled).

11. (Original) The data compilation system of claim 7 further comprising:

a) a display coupled to the data parser; and

b) a relational database coupled between the data parser and the display, and wherein: the data parser transfers the categorized data to the relational database.

12. (Original) The data compilation system of claim 11 wherein: the relational database receives a data query, and the display shows a portion of the categorized data, up to and including all the data, from the relational database, corresponding to the data query.

13. (Original) The data compilation system of claim 12 wherein: the data queries are submitted and the portions are shown through a web browser interface.

14. (Currently Amended) The data compilation system of claim 7 further comprising: a) an event detector coupled to the data parser and wherein: the event detector compares the categorized data to a predetermined event definition and provides ~~a signal~~ an event indication when [if] a match is found.

15. (Original) The data compilation system of claim 7 further comprising: a) an information technology agent and wherein: the network component is programmed by software, the agent collects security data from the software, and the data provided from the first network component is the security data collected by the agent.

16. (Original) The data compilation system of claim 7 wherein: the data parser produces formatted and categorized data.

17. (Original) The data compilation system of claim 7 wherein: data from the first network component is security data and data from the second network component is security data.

18. (Original) The data compilation system of claim 7 wherein: data from the first network component is encrypted and decrypted.

19.-26. (Canceled)

Allowable Subject Matter

Claims 1, 3-9, and 11-18, are allowed, and hereby renumbered 1-16. The record is clear as to the reasons for allowance. Accordingly, no additional statement is necessary.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Examiner's Remarks

Examiner formally withdraws the rejection under 35 USC 101 and the double patenting rejection. Applicant's newly submitted specification and abstract of December 3, 2008 has been placed in Applicant's record.

Other Prior Art Made of Record

The prior art made of record and not relied upon is considered pertinent to Applicant's disclosure. U.S. patents and U.S. patent application publications will not be supplied with Office actions. Examiners advises the Applicant that the <u>cited</u> U.S. patents and patent application publications are available for download via the Office's

PAIR. As an alternate source, all U.S. patents and patent application publications are available on the USPTO web site (www.uspto.gov), from the Office of Public Records and from commercial sources. For the use of the Office's PAIR system, Applicants may refer to the Electronic Business Center (EBC) at http://www.uspto.gov/ebc/index.html or 1-866-217-9197.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Diane D. Mizrahi whose telephone number is 571-272-4079. The examiner can normally be reached on Monday-Thursday (9:30 - 4:30 p.m.).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Christian Chase can be reached on (571) 272-4190. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 872-9306 for regular communications and (703) 305-3900 for After Final communication.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.qov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll free).

/Diane Mizrahi/

Diane.Mizrahi@USPTO.gov
Primary Patent Examiner
Technology Center 2100

December 3, 2008